ORIGINAL

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	93-292
	)	
Policies and Rules Concerning Toll Fraud	)	CC Docket NO. 93-292
	)	

Comments of O'Brien Engineering, P.C.

O'Brien Engineering, P.C., with offices at 220 Maple Avenue, Suite 205, Rockville Centre, New York 11570, is a Telecommunications Consulting Engineering Company with clients that will be affected by this Rulemaking and is therefore interested in these proceedings. The following comments have been submitted in response to the Notice of Proposed Rule Making (NPRM) in connection with CC Docket No. 93-292 In the Matter of Policies and Rules Concerning Toll Fraud released December 2, 1993.

Comments

1. **Carriers should be encouraged or required to provide at reasonable rates, blocking services to prevent calls from being completed to specific countries, or conversely, allowed to complete calls to specific countries.** High risk customer's could then specify blocking or allowed lists of countries and thereby limit fraud exposure.

2. In situations involving fraudulent telephone charges, a customer's first warning is often the fraudulent charges appearing on a telephone bill. Quite frequently such charge do not appear on the bill for the current billing period and may be delayed one or more billing cycles. The untimeliness of billing can effec-

tively increase the period of exposure for the customer.

For situations in which charges for fraudulently placed calls appear on bills after the appropriate "current" billing cycle, the customer's liability should be reduced.

3. Carriers unanimously refer to fraud as involving calls placed by "outside" parties penetrating a customer's network. This is typically achieved by hacking through DISA, voice mail, voice response units, call forwarding or other arrangements that when insecurely configured will facilitate the unauthorized connection of an incoming caller to an outgoing line. Carriers unanimously preclude from the definition of fraud, calls arising from "on premises" use of a customer's telephone system.

It is acknowledged that in most cases charges resulting from calls placed using compromised authorization codes, from unauthorized use of a telephones and from similar actions constitute abuse and are outside the scope of this proceeding. However, for institutions such as universities, hotels and hospitals which have a large degree of more "transient" users, there is a real exposure to fraud originating internally. Quite frequently such fraud involves exploiting a "Systems" problem, or an interaction of a customer's telephone system with a weakness in the public telephone network as discussed below in item 7.

The rules formulated for fraud need to address the reality that fraud may originate from on-premises use of a customer's telephone system, particularly with respect to interactions with a weakness in carriers' switching systems.

4. Carriers have the ability to rapidly detect and disable compromised calling cards. In a case investigated by this firm, calls to international destinations were placed via a compromised card number from telephones on a customer's PBX. The carrier apparently detected the problem and then attempted to bill the calls as if they had originated on a direct dial basis from the customer's telephone system within the current billing cycle. The carrier was not the pre-subscribed carrier and the line number that was billed did not have 10xxx dialing capability. The charges were contested and subsequently removed from the bill. **Rules need to be formulated to prevent this type of activity; or conversely, to uniquely identify all such "adjusted" charges on telephone bills.**

5. **FCC Part 68 Rules involving Registration should be expanded to address telephony issues that will predictably result in an insecure calling arrangement.** A classical example involves the use of loop start, as opposed to ground start Central Office lines in telephone systems or other devices such as call diverters that have the ability to patch or "forward" an incoming line to an outgoing line as described below.

> There is no standard release signal on loop start lines. Although some Central Offices provide a brief interruption of loop current, which can be construed as a disconnect signal by some CPE, this signal is unreliable. For example, it will not be passed by subscriber carrier systems that may be in place today or in the future. Unless the Central Office is arranged to block regenerated dial tone or use rotary dialing while blocking touch tone dialing, by definition,

the use of CPE with loop start lines to effect the forwarding of an incoming CO line, through the CPE and out on a second loop start CO line to an external number, is potentially insecure. After the called party hangs up, regenerated dial tone from the outgoing line will be patched through the CPE to the incoming caller. Some CPE with dial tone detection capability may be able to use the regenerated dial tone as a release signal to improve security, but the absolute reliability of this is arguable.

In the above situation, Registration could address allowable types of central office line service (e.g. loop start with regenerated dial tone blocked, or preferably, ground start lines to ensure availability of a disconnect signal).

6. The issues related to Payphone Fraud involve charges improperly billed to the payphone provider despite the existence of OLS and BNS call screening arrangements to prevent such charges. Consideration is being given to releasing a payphone provider from liability for charges from certain types of fraudulent calls if the provider purchases the appropriate call screening.

The arguments to release payphone providers from liability are valid. We agree with this position. Furthermore we propose that other customers such as aggregators who deploy the same types of screening arrangements, to protect against the same types of improperly billed calls, should logically be extended the same level of protection. If the screening services work, they work the same for all customers, not just for one class of customer.

7. The following is a brief description of several CPE Regis-

tration and "Systems" issues related to security and involving the interaction of CPE and Central Offices:

a. # End of Dialing on 0 Prefixed Calls

Due to the variable number of digits in zero prefixed calls including 0, 01 and 011 (or 10xxx + zero prefixed calls), it is difficult for the telephone system and the CO to "agree" when dialing is complete. Using circuitous dialing procedures, a caller may be able to place an IDDD call, yet the telephone system's Call Detail Recording (CDR) may show only an operator call.

The number of digits for operator or international calls is variable, so both the telephone system and the CO rely on expiration of inter-digital timing or receipt of "#" as an end of dialing indicator. If a caller dials 0 or 0#, the telephone system seizes a trunk, sends 0 and "cuts through" the connection. Before the CO's inter-digital timer expires, using tone dialing, the caller may be able to dial 11, country code, etc. to place an international call. CDR registers "0". In other variations, the caller dials 01 or 011 and waits for cut through.

The best protection is provided when the telephone system transmit "#" as the last digit on 0, 01, and 011 calls; and the CO recognizes this and stops collecting digits, ensuring that the PBX's CDR and the actual call destination are the same.

A "systems" problem occurs when the PBX correctly transmits the # end of dialing indicator, but the CO fails to recognize it. For example, Northern Telecom's DMS250 CO, when directly connected to a customer's PBX via dedicated trunks, failed to respond to

"#" as an end of dialing indicator until the problem was corrected in May 1992 via a software change made as a result of a complaint initiated by an affected customer.

b. Inconsistent Digit Treatments for * and Other Tone Digits

Some PBX's accept * as if it were a normal digit and transmit it to the CO as part of the dialed number. The CO should treat * as well as other non numeric tone digits as inconsistent digits and give an intercept announcement.

Some CO's are improperly arranged to ignore *. If the CO ignores *, a caller could dial 201-468-999* to stuff the CDR record, and then manually use cut through dialing to complete the call. The resultant CDR record will fail edit checks on most billing systems due to non numeric character in the telephone number. This problem affects end offices as well as IXC offices connected to a PBX via dedicated access facilities.

Instead of intercepting or ignoring the * digit, one type of CO switching system responds in a non standard manner that creates a significant security exposure to the end customer. The manufacturer was advised by IXC's more than two years ago, but has reportedly taken the position that the system operates in conformance with its specifications. This is another example of a "systems" problem.

In particular, Registration requirements should be formulated to ensure that systems with automatic routing correctly transmit # and respond to "inconsistent" digits to preclude the above described problems. In general, the Registration program should be expanded to address relevant security issues.

Furthermore, it is recommended that this Rulemaking address the

appropriate assignment of liability for situations involving security loopholes created by a weakness or non conforming operation in a carrier's switching system.

Conclusion

O'Brien Engineering wishes to indicate its support for the objectives expressed in the NPRM and hopes that the comments submitted herein are helpful and can be addressed in this proceeding.

Respectfully submitted,

John J. O'Brien 1/13/94

John J. O'Brien, P.E.
O'Brien Engineering, P.C.
220 Maple Avenue - Suite 205
Rockville Centre, NY 11570
(516) 536-2480